

crt.sh Certificate Search

Criteria

ID = '5950129476'

crt.sh ID	5950129476																																				
Summary	Precertificate																																				
Certificate Transparency	Log entries for this certificate: <table><thead><tr><th>Timestamp</th><th>Entry #</th><th>Log Operator</th><th>Log URL</th></tr></thead><tbody><tr><td>2022-01-10 09:43:22 UTC</td><td>491033512</td><td>Google</td><td>https://ct.googleapis.com/logs/argon2022</td></tr><tr><td>2022-01-10 09:43:22 UTC</td><td>212163987</td><td>DigiCert</td><td>https://yeti2022-2.ct.digicert.com/log</td></tr><tr><td>2022-01-10 09:43:22 UTC</td><td>581610991</td><td>Sectigo</td><td>https://mammoth.ct.comodo.com</td></tr></tbody></table>	Timestamp	Entry #	Log Operator	Log URL	2022-01-10 09:43:22 UTC	491033512	Google	https://ct.googleapis.com/logs/argon2022	2022-01-10 09:43:22 UTC	212163987	DigiCert	https://yeti2022-2.ct.digicert.com/log	2022-01-10 09:43:22 UTC	581610991	Sectigo	https://mammoth.ct.comodo.com																				
Timestamp	Entry #	Log Operator	Log URL																																		
2022-01-10 09:43:22 UTC	491033512	Google	https://ct.googleapis.com/logs/argon2022																																		
2022-01-10 09:43:22 UTC	212163987	DigiCert	https://yeti2022-2.ct.digicert.com/log																																		
2022-01-10 09:43:22 UTC	581610991	Sectigo	https://mammoth.ct.comodo.com																																		
Revocation	<table><thead><tr><th>Mechanism</th><th>Provider</th><th>Status</th><th>Revocation Date</th><th>Last Observed in CRL</th><th>Last Checked (Error)</th></tr></thead><tbody><tr><td>OCSP</td><td>The CA</td><td>Check</td><td>?</td><td>n/a</td><td>?</td></tr><tr><td>CRL</td><td>The CA</td><td>Unknown (Expired)</td><td>n/a</td><td>n/a</td><td></td></tr><tr><td>CRLSet/Blocklist</td><td>Google</td><td>Not Revoked</td><td>n/a</td><td>n/a</td><td>n/a</td></tr><tr><td>disallowedcert.stl</td><td>Microsoft</td><td>Not Revoked</td><td>n/a</td><td>n/a</td><td>n/a</td></tr><tr><td>OneCRL</td><td>Mozilla</td><td>Not Revoked</td><td>n/a</td><td>n/a</td><td>n/a</td></tr></tbody></table>	Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)	OCSP	The CA	Check	?	n/a	?	CRL	The CA	Unknown (Expired)	n/a	n/a		CRLSet/Blocklist	Google	Not Revoked	n/a	n/a	n/a	disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a	OneCRL	Mozilla	Not Revoked	n/a	n/a	n/a
Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)																																
OCSP	The CA	Check	?	n/a	?																																
CRL	The CA	Unknown (Expired)	n/a	n/a																																	
CRLSet/Blocklist	Google	Not Revoked	n/a	n/a	n/a																																
disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a																																
OneCRL	Mozilla	Not Revoked	n/a	n/a	n/a																																
Certificate Fingerprints	SHA-256 AEC0D34125434BEB0322D625108726DB8CF563082F683572174D595410A59082 SHA-1 C2381046FE98D12292A1D4A0D437A878E04BACED																																				
ASN.1 Certificate Graph Hierarchy pv Hide metadata Run cablint Run x509lint Run zlint Download Certificate: PEM Certificate: Data: Version: 3 (0x2) Serial Number: 03:ce:80:78:fd:b7:69:2f:56:f8:0e:42:c6:34:7c:98:6d:d7 Signature Algorithm: sha256WithRSAEncryption Issuer: (CA ID: 183267) commonName = R3 organizationName = Let's Encrypt countryName = US Validity (Expired) Not Before: Jan 10 08:43:22 2022 GMT Not After : Apr 10 08:43:21 2022 GMT Subject: commonName = dpat.bbdu.ac.in Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public-Key: (4096 bit) Modulus: 00:b1:65:5d:58:6c:b3:fd:a3:ed:af:89:dc:3d:ea: e1:6f:99:6a:b4:4f:39:f7:f2:4d:1d:bf:c1:53:a6: 98:27:dc:28:90:a7:9c:0e:45:1c:df:3b:23:1a:7b: a0:16:f8:d1:64:ab:a6:42:df:32:dc:43:69:67:40: ee:22:a8:49:7a:a4:0f:ad:b5:37:a5:d3:fa:80:83: 8a:bb:00:f1:78:71:de:ec:f4:74:42:6e:c8:cd:f8: 70:24:4e:f1:07:06:1e:ae:f6:e5:7f:aa:22:e3:61: 0f:31:e4:23:e6:e1:69:e3:e1:12:ff:0f:90:20:7f: fe:29:f3:5a:dd:6f:da:fd:0d:12:50:6d:79:e0:f6: 9a:92:78:44:b0:f3:0b:19:d1:d5:ad:a3:b2:6d:f8: 58:d0:f3:71:92:32:2f:a4:3f:0c:64:65:c9:34:30: e5:a3:61:bb:fc:ee:a7:aa:8e:2a:d3:19:d6:94:8a: 49:66:27:75:f1:72:ae:ae:7c:aa:da:5e:48:ab:37: cc:79:c3:31:8a:79:d9:f9:33:8a:ae:8a:dc:8e:3c: 46:ac:d5:35:38:67:56:49:3f:e8:83:89:70:3a:f6: 55:46:b2:43:72:57:6d:dd:25:c8:b0:d8:b0:ac:c2: 97:2b:d3:28:79:eb:a4:b1:a9:f5:34:a5:65:ee:d0: ef:d2:5a:b7:77:52:81:df:2c:90:ff:8b:8b:50:43: b2:d3:d3:db:be:8d:4b:91:af:06:52:5a:3a:35:e9: f9:0c:86:30:61:e9:4d:fe:a0:7d:35:76:71:a8:30: f0:ca:68:30:07:67:16:99:5a:28:c6:31:47:29:c3: 37:2a:94:00:a8:59:e8:b0:bd:66:cc:38:2e:89:97: a7:84:4b:6f:aa:f2:1f:42:eb:16:8a:56:f7:79:1d: e9:8c:95:99:6a:9c:89:21:51:aa:c2:6f:05:0a:26: 4e:dc:a5:0f:87:e6:4c:74:76:61:69:ca:87:78:44: 23:8d:8b:5e:df:e0:04:ca:77:06:2f:0e:90:38:be: d2:c0:94:73:b9:ef:43:7f:20:26:7f:47:13:c9:00: 6b:51:52:15:6f:0b:b5:23:a2:d3:16:d7:2f:45:be: 19:f7:7f:a1:d8:c3:b4:63:4c:78:08:83:08:80:e6: a9:6a:df:22:09:80:c9:21:6e:34:2a:5d:a2:99:54: 5e:9e:49:98:10:82:17:5d:f2:31:c7:3d:c4:e8:de: b2:cb:64:51:d8:1f:56:8c:c2:78:8f:36:2c:62:ea: 3e:72:f2:25:dc:e5:72:0e:d1:f6:fd:8a:f1:64:9a: d0:00:06:e9:a1:94:d6:20:3c:29:22:0e:a9:c8:63: aa:4a:1d Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Key Usage: critical Digital Signature, Key Encipherment X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 8D:85:EC:BA:E4:2A:E1:A0:1A:AA:0E:33:CB:A9:28:EB:6D:5A:15:6F X509v3 Authority Key Identifier: keyid:14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6 Authority Information Access: OCSP - URI:http://r3.o.lencr.org																																					

```
CA Issuers - URI:http://r3.i.lencr.org/

X509v3 Subject Alternative Name:
  DNS:dpat.bbdu.ac.in
X509v3 Certificate Policies:
  Policy: 2.23.140.1.2.1
  Policy: 1.3.6.1.4.1.44947.1.1.1
  CPS: http://cps.letsencrypt.org

CT Precertificate Poison: critical
NULL
Signature Algorithm: sha256WithRSAEncryption
62:90:b4:75:cb:c6:99:56:06:ff:65:85:ea:96:2d:db:3d:1d:
d2:d3:d4:ab:46:f7:57:c7:73:5a:06:48:78:87:f3:75:c8:69:
d2:93:2b:63:a4:15:c1:39:ae:cf:d4:a4:a3:f4:c0:f7:40:77:
0f:25:b6:29:13:0b:b8:7c:1a:82:e2:39:af:e5:67:4c:57:2a:
ec:5f:e3:11:0f:1c:78:71:ab:7f:d8:be:86:8a:df:5b:80:69:
6c:9d:44:02:91:55:02:e2:84:cf:04:b4:fc:1b:7d:15:2c:01:
58:34:a6:c2:5a:9d:35:2a:94:ce:3e:df:2e:bf:f3:61:f0:bb:
a2:72:78:74:fc:ce:f9:31:cb:47:81:68:f4:22:19:a7:c1:bf:
61:5b:4b:71:9d:3b:80:2a:ca:bc:12:ca:71:7b:ce:a7:32:fb:
7f:fc:08:f2:0a:7e:94:01:7a:65:0b:58:39:1c:02:11:ca:1f:
02:0a:9e:e0:ea:3c:2c:c9:5f:48:7c:6e:0b:0a:f0:fe:fd:4d:
f7:e5:0d:0c:61:09:4f:c6:b9:c1:c7:8c:b4:12:ea:74:9d:cd:
98:e7:a8:2c:03:b7:b1:f1:79:2d:80:9c:c5:94:5b:2e:c2:e3:
1f:08:8d:c6:9c:5b:33:58:52:23:3d:d5:93:7c:52:55:bd:49:
47:51:23:0f
```

© Sectigo Limited 2015-2022. All rights reserved.

